Nos. 07-21 and 07-25

In The Supreme Court of the United States

WILLIAM CRAWFORD, *ET AL.*,
Petitioners,

v.

MARION COUNTY ELECTION BOARD, *ET AL.*,
Respondents.

INDIANA DEMOCRATIC PARTY, *ET AL.*,
Petitioners,

v.

TODD ROKITA, *ET AL.*,
Respondents.

On Writs of Certiorari to the United States Court of Appeals for the Seventh Circuit

BRIEF OF THE RUTHERFORD INSTITUTE, AMICUS CURIAE, IN SUPPORT OF PETITIONERS WILLIAM CRAWFORD, ET AL. [Impact on Voters' Privacy]

John W. Whitehead
Counsel of Record
David B. Cadell
Christopher F. Moriarty
THE RUTHERFORD INSTITUTE
1440 Sachem Place
Charlottesville, Virginia 22906
(434) 978-3888

Counsel for Amicus Curiae

LANTAGNE LEGAL PRINTING
801 East Main Street Suite 100 Richmond, Virginia 23219 (800) 847-0477

QUESTION PRESENTED

Whether provisions of an Indiana state statute requiring voters to provide photo identification before they vote is unconstitutional on the grounds that it violates voters' rights under the First and Fourteenth Amendments?

TABLE OF CONTENTS

Question Presented i

Table of Contents ii

Table of Authorities iii

Interest of Amicus Curiae 1

Statement of Facts 2

Summary of Argument 3

Argument 6

I. The State Of Indiana's Photo ID Requirement Creates A Ripe Potential For Breach Of Privacy, And This Potential Will Be Increased If Real ID is Required To Vote 6

A. Privacy Concerns Today Over Voter ID 6

B. Privacy Concerns In Light Of The Commission On Federal Election Reform's Recommendations 8

Conclusion 15

TABLE OF AUTHORITIES

CASES

Crawford v. Marion County Election Board, 472 F.3d 949 (7th Cir. 2007) 3

Crawford v. Marion County Election Board, 484 F.3d 436 (7th Cir. 2007) 6

Greidinger v. Davis, 988 F.2d 1344 (4th Cir. 1993) 8

Harper v. Virginia Board of Elections, 383 U.S. 663 (1966) 3

STATUTES

Indiana Public Law 109-2005 2

U.S. Const. amends. XV, § 1 3

REAL ID ACT Pub. Law. No. 109-13, 119 Stat. 231 ..... 4, 13

Pub. Law. No. 89-110; 79 Stat. 437 (1965) 4

Intelligence Reform and Terrorism Prevention Act of 2004, § 7214, Pub. Law. No. 108-458; 118 Stat. 3638 (2004) 5

Confidentiality of Driver's License Information, California Civil Code 1798.90.1 12

Storage or Compilation of Information, Revised Statutes of Nebraska 60-4,111.01 (2001) 12

Drivers' Licenses Prohibitions, New Hampshire Revised Statutes, Title XXI, Motor Vehicles, Chapter 263, Section 263:12 12

Electronically Readable Information, Texas Statutes, Transportation Code, Title 7 Vehicles and Traffic, Chapter 521 Driver's Licenses and Certificates, Section 521.126 12

OTHER

Justin Levitt and Andrew Allison, *Reported Instances of Voter Caging* (June 2007) 3

Building Confidence in U.S. Elections, §2.5, Report of the Commission on Federal Election Reform (Sept. 2005) 4

M. Keller, David Mertz, Joseph Lorenzo Hall and Arnold Urken, *Privacy Issues in an Electronic Voting Machine* 5

Twelve Senators Urge Frist To Keep Real ID Act Off Supplemental Appropriations Bill, Press Release, S. Comm. on Homeland Sec. & Governmental Affairs (Apr. 12, 2005) 9

Arshad Mohammed and Sara Kehaulani Goo, "Government Increasingly Turning to Data Mining," *The Washington Post* (June 15, 2006) 10

Robert C. Johnston, "15 states link school status, student driving," *Education Week* (November 6, 1996) 10

Daniel J. Steinbock, *National Identity Cards: Fourth and Fifth Amendment Issues*, 56 FLA. L. REV. 697, 740 (Sept. 2004) 11

Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, Comments of Electronic Privacy Information Center 12, 13, 14

TJX Cos., Annual Report (Form 10-K), at 8-10 (Mar. 28, 2007) 13

Transportation Code, Title 7 12

INTEREST OF AMICUS CURIAE[1]

The Rutherford Institute is an international civil liberties organization headquartered in Charlottesville, Virginia. Founded in 1982 by its President, John W. Whitehead, the Institute specializes in providing legal representation without charge to individuals whose civil liberties are threatened or infringed upon and in educating the public about constitutional and human rights issues. Attorneys affiliated with the Institute have filed *amicus curiae* briefs in this Court on numerous occasions. Institute attorneys currently handle over one hundred cases nationally, including many cases that concern the interplay between the government and its citizens.

One of the purposes of The Rutherford Institute is to work to preserve one of the most basic freedoms our Republic affords its citizens—the right to vote without intimidation or discrimination. We are also dedicated to preserving Americans' constitutional right to privacy, particularly in today's digital age.

---

[1] Counsel of record to the parties in this case have consented to the filing of this brief, and letters of consent have been filed with the Clerk pursuant to Rule 37. No counsel to any party authored this brief in whole or in part.

STATEMENT OF FACTS

Respondent State of Indiana passed a voter identification law in 2005 that requires voters to produce a valid photo ID in order to vote. Indiana Public Law 109-2005. The law does not specify acceptable types of ID, but it does define the characteristics of an ID valid for voting purposes in IC 3-5-2-40.5. The ID must:

1. Display voter's photo.

2. Display voter's name, and the name must conform with the name on the voter registration record (conform does not mean match identically).

3. Contain an expiration date and either be current or have expired after November 7, 2006 (the date of the last General Election).

4. Be issued by the State of Indiana or the U.S. government.[2]

This requirement applies to all poll voters, with the exception of nursing home residents where a poll booth is located there.[3] The requirement does not apply to absentee ballots.[4]

Not all citizens of the State of Indiana currently have the identity documents that would be needed in order to vote.

---

[2] *Available at* http://www.in.gov/sos/elections/hava/2007%20Media%20Kit/Photo%20ID%20fact%20sheet.pdf.

[3] IC 3-11-8-25(e).

[4] IC 3-11-10-1.2.

SUMMARY OF ARGUMENT

This case has the potential to have a critical impact on the voting rights of all American citizens and the ease with which they can exercise their right to vote.[5] This case will have the greatest effect on minority groups, as they are the segments of society that are least likely to be able to comply with the requirements of the new law. This is because members of minority groups are less likely to have the ID required by the new law.[6]

There has been a long history of disenfranchisement in the United States, particularly of minorities. Since certain groups—primarily African-Americans—have had the legal right to vote, various methods have been used to disenfranchise them. Intimidation, literacy tests and the poll tax are among the most blatant methods that have been used in an attempt to circumvent the right of minorities to vote.

Present-day disenfranchisement has come through more subtle methods, such as voter caging, which has primarily been used to target minority residences.[7] Despite the success of the Voting Rights

---

[5] While there is no explicit constitutional right to vote, this Court has recognized that "once the franchise is granted to the electorate, lines may not be drawn which are inconsistent with the Equal Protection Clause of the Fourteenth Amendment." *Harper v. Virginia Board of Elections*, 383 U.S. 663, 665 (1966). Additionally, U.S. Const. amends. XV, § 1; XIX; and XXIV, § 1 prohibit discrimination in voting on the grounds of race, sex and age respectively.

[6] *Crawford v. Marion County Election Bd.*, 472 F.3d 949, 951 (7th Cir. 2007).

[7] *See* Justin Levitt and Andrew Allison, *Reported Instances of Voter Caging* (June 2007), *available at*

Act of 1965,[8] it would be naïve to think that attempts to disenfranchise groups in society do not still exist.

If the photo ID requirement is upheld, it would also open the door for the implementation of voter ID laws more restrictive than the State of Indiana's. The Commission on Federal Election Reform ("the Carter-Baker Report") recommends that states require "Real ID"[9] as the only acceptable form of voter identification. Enactment of this recommendation would place an even greater burden on voters than the Indiana law.[10] The success of Indiana's law would thus represent a first step in a trend of making voting more difficult, as the acceptability of drivers' licenses and even U.S. passports would disappear under the Carter-Baker Report's recommendation. Like Indiana's voter ID law, Real ID requirements would have a disproportionate burden on minority groups.

Moreover, as well as impacting on voting rights, photo ID in general—and Real ID in particular—presents significant privacy concerns. Photo identification often contains far more information than that necessary to comply with the voting requirements. For example, the Indiana driver's license contains the address of the holder,

---

http://www.brennancenter.org/dynamic/subpages/download_file_19609.pdf.

[8] Pub. Law. No. 89-110; 79 Stat. 437 (1965).

[9] REAL ID Act, Div. B Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, Pub. Law. No. 109-13, 119 Stat. 231 (May 11, 2005).

[10] *Building Confidence in U.S. Elections*, §2.5. Report of the Commission on Federal Election Reform (September 2005), *available at* http://www.american.edu/ia/cfer/report/report.html#sect2_5.

information about the holder's height and weight, and the holder's driver's license number.[11] Some older licenses also contain the holder's Social Security number, as the prohibition on states displaying Social Security numbers on drivers' licenses only went into effect on December 17, 2005.[12] Disclosing sensitive information to a poll worker—a stranger—when showing the photo ID is a considerable breach of the voter's privacy. Furthermore, in an age when privacy rights are already being impacted upon by the regular requirement to identify oneself, the necessity to produce photo ID when engaging in a fundamental right represents another step toward a "show your papers" society.

Concerns already exist over the privacy of electronic voting machines,[13] but the fact that Real ID cards will be machine-readable creates an even greater concern as to whether sensitive information could be read from the ID if it is swiped at the polling station.

Other threats—legal and illegal—would be greatly enhanced by the introduction of the Real ID card. The vast database and biometric nature of the card would be open to abuse by the thousands of state and federal employees who have access to it. "Hacking" and "skimming" of our personal data

---

[11] *See* example *at* http://www.indygov.org/NR/rdonlyres/998B3B85C-63AD-4DD4-B5BE-1602C9A33BDC/0/2007PhotoIDCardExamples.pdf.

[12] Intelligence Reform and Terrorism Prevention Act of 2004, § 7211, Pub. Law. No. 108-458; 118 Stat. 3638 (2004)

[13] *See* M. Keller, David Mertz, Joseph Lorenzo Hall and Arnold Urken, *Privacy Issues in an Electronic Voting Machine*, *available at* http://gnosis.cx/publish/voting/privacy-electronic-voting.pdf.

would be especially appealing to criminals—particularly in an age of electronic identity theft—given the completeness of the data stored on the database.

ARGUMENT

I. The State Of Indiana's Photo ID Requirement Creates A Ripe Potential For Breach Of Privacy, And This Potential Will Be Increased If Real ID Is Required To Vote.

The State of Indiana chose to turn a blind eye to the basic and fundamental right to vote and the right to privacy when it passed a law requiring citizens to produce photo ID in order to vote. This measure, which is purportedly designed to combat voter fraud,[11] undermines these basic rights and therefore should be struck down by this Court.

The requirement of the production of photo ID to vote has considerable privacy implications and represents the start of a slippery slope, particularly in light of the Carter-Baker Report's proposal that Real ID be the only acceptable form of identification for voting.

A. Privacy Concerns Today Over Voter ID

The necessity of providing photo ID at the polling station creates concerns about the individual's privacy. In particular, the individual

---

[11] The State of Indiana has been unable to identify a single instance of in-person voter fraud having ever occurred in Indiana. *Crawford v. Marion County Election Bd.*, 484 F.3d 436, 439 (7th Cir. 2007).

does not solely disclose the absolutely necessary details—her name and proof of citizenship—when she produces her ID card. The most common form of photo ID is a driver's license, which, in Indiana, contains such sensitive information as the voter's driver's license number, date of birth, height and weight.[15] Some older licenses still contain the holder's Social Security number.[16] This information is not being given to law enforcement officials or government employees but to poll workers—many of whom may be volunteers for that day only—who have no right or need to know such information. The requirement that a voter give such sensitive information to a stranger places an undue hardship on the voter's exercise of her right to vote. Furthermore, there are many citizens who, for perfectly innocent reasons, don't want to divulge their personal information to strangers. Protected witnesses and abused wives hiding from their abusive husbands are two more obvious examples of such citizens. Women with protective orders are often exempt from the publicly available address requirements on voter registration lists, so having to show IDs that contain their addresses would be particularly burdensome on their right to vote.

Significant concerns already exist about the security and privacy of electronic voting machines. Every time a ballot is cast, the voting system adds an entry to one or more software or firmware logs that consists of a timestamp and an indication that a ballot was cast. If the timestamp log is combined with the contents of the ballot, this information becomes much more sensitive. For example, it can be

---

[15] *Supra*, note 11.

[16] *Supra*, note 12.

combined with information about the order in which voters voted to compromise the confidentiality of the ballot. This information can be collected at the polling place using either overt or covert surveillance equipment, such as cell phone cameras or security cameras.[17]

Voting and privacy should, as much as possible, be mutually inclusive. Any requirement that impacts upon the secrecy of the ballot undermines the voting process. Indeed, the Fourth Circuit has advised against allowing statewide latitude in the use of personal information in elections. In *Greidinger v. Davis*, 988 F. 2d 1344, 1355 (4th Cir. 1993), the Fourth Circuit limited the scope of use of Social Security numbers in the administration of elections, holding that the publication of Social Security numbers created "an intolerable burden" on the right to vote.

Consequently, as the law stands today, there are considerable threats to the privacy rights of voters, which have been expanded by the necessity of requiring the voter to produce photo ID.

B. Privacy Concerns In Light Of The Commission on Federal Election Reform's Recommendations

In light of the Carter-Baker Report's recommendations for improvements to the electoral process, even more significant privacy concerns have arisen. One recommendation that the Commission proposed was that Real ID cards be the only form of identification acceptable in order for American

---

[17] *Supra*, note 13, at 4.

citizens to vote.[18] Real ID cards are uniform, biometric identity cards linked to databases. The Real ID card would include a 2D barcode as its machine-readable technology, allowing information to be recovered from the database on production of the Real ID card.[19] The Federal Government mandates that states be given a time extension to replace drivers' licenses and photo ID cards with Real ID versions by December 31, 2009.[20]

Some of the privacy concerns about the impact of Real ID have already been debated in the Senate, where twelve senators urged that Real ID be kept off the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief Act of 2005. They believed that Real ID "places an unrealistic and unfunded burden on the state governments and erodes Americans' civil liberties and privacy rights."[21]

The requirement of producing photo ID raises concerns about the secrecy of the ballot, particularly considering the likelihood of Real ID becoming the only acceptable form of voter ID in the future if Indiana's law is upheld. Even if it is accepted that the need to prove one's identity and citizenship

---

[18] *Supra*, note 10.

[19] *REAL ID Proposed Guidelines: Questions & Answers*. Department of Homeland Security. *available at* http://www.dhs.gov/xprevprot/laws/gc_1172767635686.shtm.

[20] *Id.*

[21] *Twelve Senators Urge Frist To Keep Real ID Act Off Supplemental Appropriations Bill*. Press Release, S. Comm. on Homeland Sec. & Governmental Affairs (Apr. 12, 2005). *available at* http://www.senate.gov/%7Egov_affairs/index.cfm?FuseAction=PressReleases.Detail&Affiliation=R&PressRelease_id=953&Month=4&Year=2005.

through documentation in order to vote is valid, information other than that could be communicated from the biometric nature of the card, especially if electronic voting machines are used. When information is provided by biometric cards, there is a possibility that data from them will be collected and used for purposes unknown to the voter. Therefore, this will reduce voter confidence in the system.

These concerns about government control over private information are not merely illusory or hypothetical, given recent government programs designed to collect private information. The Pentagon pays a private company to compile data on teenagers it can recruit to the military. Likewise, the Department of Homeland Security buys consumer information to help screen people at borders and detect immigration fraud.[22] Fifteen states were already linking drivers' licenses with school attendance and performance a decade ago.[23]

As such, certain behaviors are already being encouraged or discouraged by the government. The biometric nature of Real ID opens the possibility for a further increase in government agency monitoring of citizens' lives, as the network necessary to support Real ID would contain large amounts of private data in numerous areas of the lives of millions of citizens.

It will no longer be just the cowboy who sees the value in being able to move through life without an obligation to identify himself. Indeed, Real ID will

---

[22] Arshad Mohammed and Sara Kehaulani Goo, "Government Increasingly Turning to Data Mining," *The Washington Post* (June 15, 2006). http://www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063.html.

[23] Robert C. Johnston, "15 states link school status, student driving," *Education Week* (November 6, 1996), p. 1.

make regular identification of oneself a necessity. The value of not having to identify oneself when one has done nothing to warrant it is similar to the value not to be stopped and searched without probable cause. The move toward greater identification of a society's citizens represents a move toward a less free society. While showing a photo ID in order to vote might only seem like a minor burden on voters' rights, this could be substantial in the longer term. As Professor Daniel J. Steinbock has stated, identity documents have "an additional subjective effect on a grand scale: the psychic harm to free people of having to 'show your papers'... Not only would people forced to go through identity checkpoints experience some degree of fear and surprise, but also knowing that this has become a permanent part of the social fabric would diminish their sense of liberty."[24]

Eventual use of the Real ID card is not the sole privacy concern with voter ID. Once the data on a government database created through voter ID has been lawfully acquired, the data are the government's property. At this point, the government can do with it as it sees fit (unless there is a law or constitutional principle to the contrary). There are numerous risks to privacy from such a database, both legal and illegal. As the Electronic Privacy Information Center has pointed out, some of these problems have already manifested themselves, with some states experiencing problems of unauthorized parties accessing license and ID card

---

[24] Daniel J. Steinbock, *National Identity Cards: Fourth and Fifth Amendment Issues*, 56 FLA. L. REV. 697, 740 (Sept. 2004).

data.[25] California,[26] Nebraska,[27] New Hampshire[28] and Texas,[29] for example, already have laws restricting the "skimming" of such data. The broad expansion of data collection and retention will create even greater risks, especially as there will be an increase in the number and type of documents retained in the database.

The Real ID system contemplates the consolidation of documents that are kept in a variety of places—the Social Security system, the immigration system, local courthouses, etc.—into

---

[25] *Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, Comments of Electronic Privacy Information Center, p.22

[26] Confidentiality of Driver's License Information, California Civil Code 1798.90.1 (Effective January 1, 2004).

[27] Storage or Compilation of Information, Revised Statutes of Nebraska 60-4,111.01 (2001). The Nebraska law limits storage or compilation of information from the license or State identification card to the statutorily authorized purposes of the DMV, the courts or law enforcement agencies. Violation of the law is a felony.

[28] Drivers' Licenses Prohibitions, New Hampshire Revised Statutes, Title XXI, Motor Vehicles, Chapter 263, Section 263:12 (Effective January 1, 2003). The law prohibits scanning, recording or storing of the personal information obtained from the license unless authorized by the department. Non-electronic transfer of the information on the face of the license is prohibited without the consent of the license holder, except to law enforcement.

[29] Electronically Readable Information, Texas Statutes, Transportation Code, Title 7 Vehicles and Traffic, Chapter 521 Driver's Licenses and Certificates, Section 521.126 (Effective September 1, 2005). The law limits access to law enforcement, to identify a voter, to financial institutions for identification purposes and only with express consent, and upon authorization of a maritime facility, to secure the facility or port.

one national database.[30] This presents a huge incentive for abuse, from both authorized and unauthorized users.

Moreover, the list of security and privacy breaches of personal cards is huge. Recently, for example, almost 46 million credit and debit card numbers were stolen by hackers who accessed the computer systems at the TJX Companies over a period of several years. This made it the biggest breach of personal data ever reported.[31]

Considering such examples of widespread abuse of computerized data in the United States, the risk for abuse of Real ID cards and the accompanying database is therefore huge. A centralized database, such as that proposed by Real ID, would be a tempting target for identity thieves, which remains the number one concern of U.S. consumers, according to the Federal Trade Commission.[32] Identity cards are already being scanned for personal information by a variety of organizations that have no legitimate claim to this information. Bars and casinos, for example, have built up vast databases on their clients by surreptitiously skimming information from drivers' licenses.[33] Considering the volume of private

---

[30] Real ID Act of 2005, § 202(d)(12); (d)(13).

[31] *Supra* note 25, at p.11, citing, TJX Cos., Annual Report (Form 10-K), at 8-10 (Mar. 28, 2007), *available at* http://ir.10kwizard.com/download.php?format=PDF&ipage=1772887&source=187.

[32] Fed. Trade Comm'n, *Consumer Fraud and Identity Theft Compliant Data: January – December 2006* (Feb. 7, 2007), http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

[33] *Bars, Casinos Swipe Personal Information from Drivers License*, thenewspaper.com, http://www.thenewspaper.com/news/11/1157.asp.

information that the Real ID card will hold, such privacy threats are of significant concern.

As well as the more obvious concern about unauthorized access is the risk that authorized users could abuse their power. A 2005 scandal in Florida highlights some of the risks associated with large database systems. There, a woman wrote to a newspaper criticizing a Florida sheriff as being too fat for police work and condemning his agency's use of stun guns. Orange County Sheriff Kevin Beary ordered staffers to use state driver's license records to find the home address of his critic. The sheriff sent her a letter at her home address, and she reported being surprised that he was able to track her down so easily.[34] Such potential for abuse is multiplied by a database that contains so much information and is accessible by thousands of state and federal employees.

Concerns about the abuse of biometric identity cards are not unique to the United States. The planned introduction of biometric ID cards in the United Kingdom has raised similar privacy concerns to those discussed. The Joint Committee on Human Rights ("JCHR") concluded that the interference in the private lives of citizens which would be brought about by an identity card would require a "pressing social need" and must not be achievable through less intrusive means.[35] The JCHR went on to express

---

[34] *Supra*, note 25, p. 45, citing, "Called fat, sheriff tracks down reader," *Associated Press*, April 6, 2005.

[35] House of Lords House of Commons Joint Committee on Human Rights, *Scrutiny: Fourth Progress Report, Eighth Report of Session 2004 05* (March, 2005), http://www.publications.parliament.uk/pa/jt200405/jtselect/jtrights/60/60.pdf.

particular concern that ID cards could build a "detailed picture of private life."[36]

As to the future of voting, serious questions arise as to why a biometric identity card is needed in order to vote. Why is the Carter-Baker Commission so adamant that this form of photographic identification be used, to the exclusion of even a passport? The Real ID card will be swiped and/or scanned, but will this be extended into the field of voting, allowing voting trends and patterns to be monitored by electronic voting machines? If Respondents are successful, there are very real dangers—or at least risks that have not been addressed—for the future of voting in the United States.

CONCLUSION

For the aforementioned reasons, the State of Indiana's photo identification requirement goes against the fundamental democratic principle of voter participation and represents a return to the disenfranchisement era of American politics. Furthermore, the attack on voters' privacy rights goes against a long American tradition of individual privacy. The Court should, therefore, affirm Petitioner's claim and reverse the Seventh Circuit's ruling.

---

[36] House of Lords House of Commons Joint Committee on Human Rights, *Fifth Report* (29th November, 2004), at point 14, http://www.publications.parliament.uk/pa/jt200405/jtselect/jtrights/35/3504.htm.

Date: November 13, 2007

Respectfully submitted,
John W. Whitehead,
Counsel of Record
David B. Caddell
Christopher F. Moriarty
The Rutherford Institute
1440 Sachem Place
Charlottesville, Virginia 22901
(434) 978-3888